IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA *v.* KRISTOPHER KNEUBUHLER	Criminal Action No. 1:23-CR-047-MHC-JEM

Government's Response in Opposition to Defendant's Motion to Suppress

The United States of America, by Ryan K. Buchanan, United States Attorney, and Theodore S. Hertzberg, Assistant United States Attorney for the Northern District of Georgia, files this Response in Opposition to Defendant's Motion to Suppress Evidence and Fruits Seized Pursuant to the Search of 300 Anchorage Place, Roswell, GA 30076. The search warrant on 300 Anchorage Place provided sufficient probable cause to establish a nexus between Defendant Kristopher Kneubuhler, the residence to be searched, and the possession of child sex abuse materials ("CSAM") in violation of federal law. The search warrant was limited to electronic devices and storage media that could be used to distribute, possess, or depict child pornography or erotica, was sufficiently particularized, and was not overbroad. Defendant's motion should be denied.

1. Factual Background[1]

On June 16, 2022, the Internet Watch Foundation informed Coinbase, a cryptocurrency exchange, that a particular website on the darkweb was selling

[1] The factual background set forth herein is derived from the allegations of the affidavit in support of the challenged search warrant. (Doc. 31-3).

access to CSAM in exchange for Bitcoin. (Doc 31-3 at 14, ¶ 22). The darkweb website indicated a particular "bitcoin address" to which funds should be sent in order to obtain access. (*Id.*). Coinbase conducted an investigation, identified an account that had sent funds to that bitcoin address, and relayed its findings to Homeland Security Investigations ("HSI"). (*Id.* at 14-15, ¶ 23). HSI then subpoenaed Coinbase for additional information regarding the account that had sent funds to the bitcoin address listed on the darkweb website at issue. (*Id.* at 15, ¶ 24).

On August 19, 2022, HSI received from Coinbase information revealing that Defendant Kristopher Kneubuhler was the owner of the account that had sent funds to the bitcoin address and for which HSI had subpoenaed additional information. (*Id.*). The information HSI received linking Defendant to the Coinbase account included Defendant's home address (300 Anchorage Place, Roswell, Georgia), an image of Defendant's driver's license, and Defendant's email address, kris@harmonic-homes.com. (*Id.*).

HSI Special Agent ("SA") Kasey Crump corroborated Defendant's association to the identifiers that Coinbase had disclosed. In doing so, SA Crump researched the "kris@harmonic-homes.com" email address that Coinbase had reported. (*Id.* at 16, ¶ 28). SA Crump learned that Harmonic Homes, LLC is a home automation and security company registered with the State of Georgia and that, according to information on a state website, that company was located at Defendant's home at 300 Anchorage Place (which was the same address Coinbase provided for the holder of the Coinbase account that transacted with the darkweb website) and was "registered to" Defendant. (*Id.*).

SA Crump also connected Defendant to the 300 Anchorage Place residence through county records, other documents, and physical surveillance. Specifically, SA Crump learned through the Fulton County Board of Assessor's website that Defendant had owned 300 Anchorage Place since 2017 and that he was the responsible party for water and sewer services to the property. (*Id.* at 17, ¶ 30). Documents SA Crump obtained from a private storage company revealed that Defendant executed a rental agreement that provided 300 Anchorage Place as his address and kris@harmonic-homes.com as his email address. (*Id.* at 16-17, ¶ 29). And, during physical surveillance in December 2022, SA Crump saw Defendant's wife and one of his children enter 300 Anchorage Place from a vehicle registered at that address to Defendant's wife. (*Id.* at 17, ¶ 31).

In addition to the information identifying Defendant Kneubuhler as the accountholder for the Coinbase account that transacted with the darkweb website and associating Defendant with 300 Anchorage Place, Coinbase provided HSI a transaction history for Defendant's Coinbase account. (*Id.* at 15, ¶ 25). That transaction history reflected the transfer of Bitcoin from Defendant's account to the bitcoin address listed on the darkweb website. (*Id.*).

Separately, HSI received from the Internet Watch Foundation a screenshot from the darkweb website listing the bitcoin address to which a person would send $89.99 in "Bitcoin equivalent" as a prerequisite to logging into the darkweb website and obtaining more CSAM. (*Id.* at 15-16, ¶ 26). Using an undercover computer in December 2022, SA Crump navigated to the darkweb website herself and observed that it remained active. (*Id.* at 16, ¶ 27). SA Crump saw multiple images and videos of CSAM on the site and that, consistent with the information

from Internet Watch Foundation, a potential could send $89.99 of Bitcoin to the bitcoin address listed on the website to access to the website's whole CSAM collection. (*Id.*).

2. Procedural History

On December 28, 2022, SA Crump applied for a warrant to search 300 Anchorage Place and to seize certain property, information, and data therein. (*Id.* at 1-22). SA Crump's application presented the facts above and explained the steps that one must follow to access websites on the darkweb and how those steps conceal the IP addresses and physical locations of a darkweb websites's host, administrator, and users. (*Id.* at 8-9, ¶¶ 17-18). SA Crump also detailed characteristics known to her that relate to individuals with a sexual interest in children, including but not limited to collecting sexually explicit images of minors and child erotica, storing such images in digital formats on a variety of devices that can store or transport any type of computer media, and keeping said collections close to them, such as in their homes or offices. (*Id.* at 6-8, ¶ 16). The affidavit in support of SA Crump's application also articulated facts regarding the interplay between computers and child pornography, the darkweb, cryptocurrency wallets, and digital currency exchangers. (*Id.* at 3-6 & 9-14, ¶¶ 5-15 & 19).

On the same day, United States Magistrate Judge Justin S. Anand granted SA Crump's application and issued the requested search warrant. (Doc. 31-2). The warrant authorized law enforcement officers to search 300 Anchorage Place, including all structures and vehicles on the property or within its curtilage, for computers and electronic devices and storage media that may be used or are use

in connection with child pornography.[2] (*Id.* at 3-4). The warrant explicitly authorized "[t]he search of such equipment" for particular items pertaining to the possession, receipt, and distribution of child pornography. (*Id.* at 4-7).

On January 5, 2023, HSI SA Crump and other agents executed the search warrant and seized fifteen electronic devices from 300 Anchorage Place. During the search, Defendant spoke with agents voluntarily and confessed to having accessed the darkweb to download CSAM, to knowing that the CSAM depicted minors engaged in sexually explicit conduct, and to storing the CSAM on a removable flash drive. (Doc. 1 at 2). Subsequent forensic analyses revealed the presence of more than 1,000 CSAM videos and images on more than a half-dozen of the seized devices. (Doc. 33-3).

On May 15, 2023, Defendant moved to suppress both the evidence seized from his home and his statements to law enforcement. (Doc. 31). In a supporting brief, Defendant argued that SA Crump's affidavit did not set forth facts establishing a nexus between the crimes alleged and the place to be searched;[3] that the affidavit failed to describe with particularity the things to be seized; and that the "good faith exception" to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984), does not apply. (Doc. 31-1).

---

[2] Specifically, the warrant was limited to computers, devices, and media "that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica." (Doc. 31-2 at 4, ¶ 1).

[3] Defendant concedes that the affidavit established the requisite nexus between himself and the place to be searched. (Doc. 31-1 at 9).

3. Argument

A. The Affidavit Established Probable Cause to Believe Evidence Related to Possession of CSAM Would Be Found at Defendant's Home.

The task of a magistrate judge issuing a search warrant "is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . , there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). The magistrate judge's determination of whether probable cause exists is made in light of the totality of circumstances. *Id.*

To establish probable cause, an affidavit should establish "a connection between the defendant and the residence to be searched and a link between the residence and any criminal activity." *United States v. Kapordelis*, 569 F.3d 1291, 1310 (11th Cir. 2009) (quoting *United States v. Martin*, 297 F.3d 1308, 1314 (11th Cir. 2002)). A realistic and commonsense approach should be employed as to encourage use of the warrant process. *United States v. Miller*, 24 F.3d 1357, 1361 (11th Cir. 1994).

In determining whether a search warrant is supported by probable cause, a reviewing court does not conduct a *de novo* determination of probable cause. *Massachusetts v. Upton*, 466 U.S. 727, 728 (1984). Rejecting "a grudging or negative attitude by reviewing courts towards warrants," the Supreme Court has made clear time and again that a "deferential standard of review" is appropriate. *Id.* at 733 (citing *Gates*, 462 U.S. at 236-37 & n.10 and *United States v. Ventresca*, 380 U.S. 102, 108 (1965)). In this circuit, reviewing courts owe "substantial deference to an issuing magistrate's probable cause determinations." *Miller*, 24 F.3d at 1363.

Magistrate Judge Anand determined correctly that SA Crump's affidavit set forth probable cause to believe evidence of CSAM possession would be found at Defendant's home. The affidavit detailed how Defendant's Coinbase account, which was associated with Defendant's home address, was used to send funds to a darkweb site selling access to CSAM. A reasonable and "practical, common-sense" inference to be drawn from those facts was that Defendant had visited the darkweb site—which, as noted in the affidavit, contained multiple images and videos of CSAM—and transferred funds from his Bitcoin wallet to obtain even greater access to CSAM. And the facts that SA Crump provided regarding the characteristics of individuals who have a sexual interest in children (which would reasonably include people like Defendant who have paid approximately $90 to access a child pornography website), supported the additional inferences that Defendant would possess the materials he paid for and that evidence pertaining to said possession was likely to be found at his home. *See, e.g.*, *United States v. Frechette*, 583 F.3d 374, 380 (6th Cir. 2009) ("[I]f someone spends $80 for something, it is highly likely that the person will use it—whether it is a tie, a video game, or a subscription to a pornographic web site."), *cited with approval*, *United States v. Schwinn*, 376 F. App'x 974 (11th Cir. 2010).[4]

[4] The affidavit explained that individuals with a sexual interest in children tend to collect child pornography and keep such images in areas they control, such as in their homes. (Doc. 31-3 at 6-7, ¶ 16). But that phenomenon need not have been articulated explicitly for the magistrate judge to make the appropriate inferences. This Court has acknowledged the "well known and recognized links between pedophilic behavior"—such as buying a subscription to a CSAM treasure trove on the darkweb—"and possession of child pornography by such individuals in secure and safe locations, such as a residence." *United States v. Lebowitz*, 647 F. Supp. 2d 1336, 1354 (N.D. Ga. 2009), *aff'd*, 676 F.3d 1000 (11th Cir. 2012). Based on

The cases Defendant cites in his motion, including *Schwinn*, are not to the contrary. In fact, in each of the Eleventh Circuit cases cited by Defendant, the court of appeals held the challenged affidavit was sufficient. *See United States v. Carroll*, 886 F.3d 1347 (11th Cir. 2018); *United States v. Lovvorn*, 524 F. App'x 485 (11th Cir. 2013); *Schwinn*, 376 F. App'x 974; *United States v. Vanbrackle*, 397 F. App'x 557 (11th Cir. 2010). Defendant endeavors to use those unfavorable cases as "contra example[s]" (Doc. 31-1 at 10), highlighting facts present there that are not present here. And he laments that SA Crump's affidavit did not proffer information about a variety of things, including IP addresses and dates Defendant accessed the darkweb site. (*Id.* at 9). But Defendant's approach is backwards; a reviewing court looks at what is in an affidavit, not what wasn't.[5] *See W. Point-Pepperell, Inc. v. Donovan*, 689 F.2d 950, 959 (11th Cir. 1982) ("[J]udicial review of the sufficiency of an affidavit for the issuance of a warrant must be strictly confined to the information brought to the magistrate's attention.").

---

that knowledge, "the magistrate judge was authorized in drawing the reasonable inference" that child pornography related materials would be found in Defendant's home. *Id.*

[5] As to Defendant's specific gripes about the affidavit's failure to connect Defendant's devices to any IP addresses used to access the darkweb site or Coinbase, SA Crump's affidavit explained how the Tor network facilitates anonymous communication over the darkweb and conceals a user's actual IP address. (Doc. 31-3 at 8-9, ¶ 17). *See also Vanbrackle*, 397 F. App'x at 560 ("Although IP address information could have definitively shown that a computer used at Vanbrackle's home received the images in question, Agent Blackwell was only obligated to provide enough facts to show a fair probability that evidence of a crime would be found at Vanbrackle's residence." (internal citation omitted)).

Moreover, omission or absence of additional information that "might have been helpful in further confirming" a defendant's involvement in a crime is irrelevant where, as here, the affidavit sets forth an adequate factual basis for a magistrate judge to find probable cause. *United States v. Bridges*, 2008 WL 11431069, at *8 (N.D. Ga. July 1, 2008) (rejecting argument that affidavit was deficient without more information about PayPal account used to purchase access to CSAM website), *report and recommendation adopted*, 2008 WL 11431071 (N.D. Ga. Sept. 2, 2008), *aff'd*, 347 F. App'x 459 (11th Cir. 2009); *see also United States v. Schwinn*, 2008 WL 782520, at *4 (M.D. Fla. Mar. 21, 2008) ("The issue before the magistrate judge in deciding whether to authorize a search warrant is not what was not in the affidavit, but whether what was in the affidavit was sufficient."), *aff'd*, 376 F. App'x 974.

Defendant's motion seems to presume that direct evidence is necessary to link the place to be searched with criminal activity. But the law is otherwise. Probable cause can be, and often is, inferred by considering the type of crime, the nature of the items sought, the suspect's opportunity for concealment, and normal inferences about where a criminal might hide the fruits of his crime. *See Lebowitz*, 647 F. Supp. 2d at 1354 (citation omitted). Based on the nature of the evidence and type of offense, a court is entitled to draw reasonable inferences about where evidence is likely to be kept. *See United States v. Lockett*, 674 F.2d 843, 846 (11th Cir. 1982) ("[T]he nexus between the objects to be seized and the premises searched can be established from the particular circumstances involved and need not rest on direct observation."). For example, this Court has often reached the commonsense conclusion in bank robbery and stolen property cases that a suspect

would stash "the loot" and other evidence at home. *See, e.g.*, *United States v. Pertha*, 2017 WL 9471691, at *4 (N.D. Ga. May 9, 2017), *report and recommendation adopted sub nom. United States v. Partha*, 2017 WL 2399579 (N.D. Ga. June 2, 2017); *United States v. Toumasian*, 2011 WL 3798223, at *7 (N.D. Ga. July 19, 2011), *report and recommendation adopted*, 2011 WL 3738980 (N.D. Ga. Aug. 22, 2011); *United States v. Gonzalez*, 2010 WL 2721882, at *16 (N.D. Ga. May 25, 2010), *report and recommendation adopted*, 2010 WL 2721540 (N.D. Ga. July 7, 2010).

Consistent with the facts presented in ¶ 16 of SA Crump's affidavit, many courts have noted that, in child pornography possession cases, evidence is likely to be found in the defendant's home, an environment the defendant believes is safe, secure, and private. Last year, in this district, Chief Magistrate Judge Russell G. Vineyard identified several of those cases:

> *[S]ee United States v. Riccardi*, 405 F.3d 852, 860-61 (10th Cir. 2005) (citation omitted) (holding that the affidavit's statement that "possessors of child pornography often obtain and retain images of child pornography on their computers," along with other facts, was "more than enough to support" probable cause); *United States v. Hay*, 231 F.3d 630, 636 (9th Cir. 2000) (reasoning that the collector profile "form[ed] the basis upon which the magistrate judge could plausibly conclude that those files were still on the premises"); *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997) (footnote and citation omitted) (finding the affidavit provided probable cause that items sought were in defendant's apartment where affiant explained that "collectors and distributors of child pornography value their sexually explicit materials highly, 'rarely if ever' dispose of such material, and store it 'for long periods' in a secure place, typically in their homes"); *United States v. Potts*, 559 F. Supp. 2d 1162, 1172 (D. Kan. 2008) (footnote omitted) (finding sufficient nexus to residence and stating that "[c]rimes involving child pornography are often tied to a secure place, like a private residence"); *United States v. Schwinn*, No. 2:07-cr-119-FtM-29SPC, 2008 WL 782520, at *3

> (M.D. Fla. Mar. 21, 2008) (finding that the totality of the circumstances allowed the magistrate judge to conclude that there was a fair probability that child pornography was in the defendant's apartment as of the date of the issuance of the search warrant), *aff'd*, 376 F. App'x 974 (11th Cir. 2010) (per curiam) (unpublished); *United States v. Johnson*, Criminal No. 07-408 (DWF/SRN), 2008 WL 465258, at *2 (D. Minn. Feb. 15, 2008) (concluding that probable cause was established for search of defendant's computers and other media located in his residence where affidavit relayed the investigation in detail, including the investigation by other agents, that at least 19 images of child pornography had been downloaded to IP addresses registered to defendant); *United States v. Cox*, 190 F. Supp. 2d 330, 333 (N.D.N.Y. 2002) (citations omitted) (noting the "observation that images of child pornography are likely to be hoarded by persons interested in [such] material [i]n the privacy of their homes is supported by common sense and the cases").

United States v. Vincent, 2022 WL 1401463 (N.D. Ga. May 3, 2022), report and recommendation adopted, 2022 WL 2452301 (N.D. Ga. July 6, 2022). Moreover, given common knowledge that individuals keep and utilize computers in their homes and the affidavit's identification of 300 Anchorage Place as both Defendant's home and place of business, Magistrate Judge Anand could reasonably infer in this case that evidence of Defendant's internet-based cybercrime would be found at 300 Anchorage Place.

The three cases Defendant cites in which affidavits were found to be lacking in probable cause—all of which were decided outside of the Eleventh Circuit—bear scant resemblance to this case. Neither *United States v. Zimmerman*, 277 F.3d 426 (3d Cir. 2002), nor *United States v. Doyle*, 650 F.3d 460 (4th Cir. 2011), involved use of the internet or a computer to obtain CSAM. In fact, *Zimmerman* did not involve a search for CSAM at all, and both cases assessed the sufficiency of affidavits in support of state warrants to search for evidence of state-law crimes. Defendant

contends that *United States v. Falso*, 544 F.3d 110 (2d Cir. 2008) is "strikingly similar" to this case, but it is anything but. In *Falso*, a sharply divided panel determined that, even though an agent's affidavit failed to establish probable cause to search the home of a person who the agent speculated was "perhaps one of several hundred possible subscribers" to a child pornography website, the good-faith exception applied, and suppression was not appropriate. *Id.* at 120-29. In that case, the FBI had forensically examined a free website that advertised a fee-based membership in a second members-only website that contained CSAM, and the examination of the free website revealed a list of email addresses including Mr. Falso's. 544 F.3d at 113-14. Unlike here, where SA Crump obtained, reviewed, and parsed records from Coinbase showing that Defendant paid for CSAM on the darkweb, the affidavit in *Falso* presented no evidence that the defendant ever purchased access to the members-only child pornography site. In *Falso*, the absence of evidence of a paid subscription was dispositive on question of probable cause, but the court of appeals noted that the outcome would have been different had the defendant's membership in the paid website been presented to the magistrate judge. Indeed, the panel cited opinions from the Third, Fifth, Sixth, Ninth, and Tenth Circuits upholding the validity of search warrants and noting that "[t]he common thread among these cases is the defendants' membership in or subscription to websites whose principal purpose was the collection and/or sharing of child pornography." *Id.* at 120 (listing cases); *see also id*. at 121 ("[M]embership in or a subscription to a child-pornography website is an important consideration in these types of cases because it supports the ultimate inference . . . that illegal activity is afoot.").

B. The Search Warrant Was Sufficiently Particularized.

To satisfy the Fourth Amendment's particularity requirement, a search warrant must "particularly describe the place to be searched, and the persons or things to be seized." *United States v. Betancourt*, 734 F.2d 750, 754 (11th Cir. 1984) (citation omitted). However, "elaborate specificity is unnecessary." *Id.* Rather, the description needs to be sufficiently particular only to enable the searcher to reasonably ascertain and identify the things authorized to be seized. *Id.* at 754–55. "Particularity is the [Fourth Amendment] requirement that the warrant must clearly state what is sought." *United States v. Maali*, 346 F. Supp. 2d 1226, 1239 (M.D. Fla. 2004), *aff'd sub nom. United States v. Khanani*, 502 F.3d 1281 (11th Cir. 2007). The reviewing court determines *de novo* whether a warrant lacked the particularity required by the Fourth Amendment. *United States v. Bradley*, 644 F.3d 1213, 1258-59 (11th Cir. 2011).

In this case, the search warrant satisfied the Fourth Amendment's particularity requirement because Attachment B, which was several pages in length, supplied enough detail to guide the executing agents' judgment in selecting what electronic items take and search.[6]

---

[6] Contrary to Defendant's claim that the warrant only authorized agents to search "for" particular devices and that their searches "of" those devices were "warrantless," the affidavit and Attachment B thereto make clear that searches of the devices themselves were authorized. First, in the closing paragraph of the affidavit, SA Crump requested that the Court "issue a warrant . . . authorizing the seizure and search of the items described in Attachment B." (Doc. 31-3 at 17, ¶ 32 (emphasis added)). And while paragraph 1 of Attachment B described the sort of devices to be seized, paragraph 2 articulated limits on "[t]he search of such equipment" (emphasis added). Moreover, the Federal Rules of Criminal Procedure state that, by default, unless otherwise specified, a warrant authorizing

Contrary to Defendant's contention that the warrant permitted a general search of his residence, the search warrant was limited to only electronic devices and storage media that could be used to distribute, possess, or depict child pornography or erotica. (Doc. 31-3 at 19, ¶ 1). And, with additional references to "child pornography," "the sexual exploitation of children," and "visual depictions of minors engaged in sexually explicit conduct," the warrant further limited agents' search of those devices for specific categories of data. (*Id.* at 19-21, ¶ 2).

Warrants less specific than the one in this case have survived scrutiny by other judges in this Court. For example, in *United States v. McDaniel*, Judge Murphy rejected a defendant's argument that a warrant authorizing the seizure of all "computer(s) and computer systems and files and contents therein" and "computer storage media/medium including hard drives, floppy discs, hard discs, compact discs (C.D.'s), zip discs, and disc drives" that might contain evidence of a violation of Georgia's electronic child pornography statute was insufficiently particularized. 2009 WL 10674310, at *3-4 (N.D. Ga. May 18, 2009). Judge Murphy law enforcement officers need not give an exact description of the materials to be seized provided that the description "is as specific as the circumstances and the nature of the activity under investigation permit." *Id.* at *8 (quoting *United States v. Santarelli*, 778 F.2d 609, 614 (11th Cir. 1985). Relevant here, Judge Murphy adopted the magistrate judge's determination that "the ubiquitous nature of personal computer equipment and digital storage media precluded [an

---

the seizure of electronic storage media or electronically stored information also authorizes a later review of the media or information. Fed. R. Crim. P. 41(e)(2)(B).

affiant] from giving a more exact description of the items to be seized." *Id.* Also, relevant here, Judge Murphy pointed out that the defendant's attack on the warrant's particularity "ignores that the warrant specifically connects the items to be seized with the criminal conduct of 'computer pornography and child exploitation." *Id.* at *9. As noted above, Paragraph 1 of Attachment B contained similar limiting language that precluded a free-ranging search.[7]

As discussed below, even if the warrant was overbroad, which was it was not, the good faith exception would still apply. *See United States v. Travers*, 233 F.3d 1327, 1330 (11th Cir. 2000) ("The good faith exception may be applied to a search conducted pursuant to an overly broad warrant.").

C. The *Leon* Good Faith Exception Applies.

If the Court was to find the search warrant invalid, either for lack of probable cause, lack of particularity, or both, suppression would not be appropriate because HSI agents acted in objectively reasonable reliance on the search warrant and the search warrant affidavit established at least an indicia of probable cause as to the nexus between Defendant, his residence, and his criminal activity.

---

[7] Cases similar to *McDonald* abound in this district. *See, e.g.*, *United States v. Carroll*, 2015 WL 13741254 (N.D. Ga. Nov. 3, 2015), *report and recommendation adopted*, 2015 WL 8491011 (N.D. Ga. Dec. 10, 2015), *aff'd*, 886 F.3d 1347 (11th Cir. 2018); *United States v. Graham*, 2014 WL 2922388 (N.D. Ga. June 27, 2014); *United States v. Wilson*, 2012 WL 7992597 (N.D. Ga. Nov. 28, 2012), *report and recommendation adopted*, 2013 WL 1800018 (N.D. Ga. Apr. 26, 2013). By contrast, Defendant has not cited a single case where a court in the Eleventh Circuit has found an affidavit comparable to SA Crump's to be overbroad.

1. Agents Reasonably Relied on the Search Warrant.

The Supreme Court has emphasized that suppression of evidence "has always been [its] last resort, not [its] first impulse." *Hudson v. Michigan*, 547 U.S. 586, 591 (2006). In *United States v. Leon*, 468 U.S. 897, 925 (1984), the Supreme Court held that evidence obtained by officers acting in objectively reasonable reliance – i.e., "good faith" – on a search warrant should not be subject to the exclusionary rule. *See also United States v. Morales*, 987 F.3d 966, 969 (11th Cir. 2021) ("The exclusionary rule exists to deter unreasonable searches, but the police here did exactly what the Fourth Amendment required of them: they obtained a warrant in good faith from a neutral magistrate and reasonably relied on it.").

The good faith exception applies where the officers "obtained and relied on a warrant from a neutral magistrate and had no reason to think that probable cause was absent despite the magistrate's authorization." *Morales*, 987 F.3d at 974. Further, when a warrant may have violated a constitutional requirement, the *Leon* exception applies to areas where it was a "close enough question" that the warrants were not "so facially deficient" that the agents who executed it could not have reasonably believed them to be valid. *United States v. Blake*, 868 F.3d 960, 975 (11th Cir. 2017).

Even if the search warrant was invalid, the *Leon* good faith exception applies because the HSI agents reasonably relied on the warrant issued by a neutral, detached magistrate judge. *See, e.g., Morales*, 987 F.3d at 974. Here, the search warrant showed a nexus between the defendant and the residence to be searched and the residence and the alleged criminal activity. Further, the search warrant limited the seizure to evidence related to the specific crime under investigation.

At a minimum, the search warrant presented a "close enough question" as to probable cause and particularity that the agents who executed the warrant could reasonably believe them to be valid. *See, e.g.*, *Blake*, 868 F.3d at 975.

2. None of the Limited Exceptions to *Leon* Apply.

Leon applies in all except in four limited circumstances. 468 U.S. at 923-24 (listing exceptions). Defendant argues only one here: that the affidavit supporting the warrant was "so lacking indicia of probable cause as to render official belief in its existence entirely unreasonable." (Doc. 31-1 at 16). Yet Defendant does not cite any case in which the Eleventh Circuit found a warrant to be so lacking. Instead, Defendant presents *Vanbrackle*, *Falso*, and *Schwinn*, where searches were upheld and motions to suppress were denied, as counterexamples. (Doc. 31-1 at 16-17).

In determining whether an affidavit lacks indicia of probable cause, a reviewing court looks only at the face of the affidavit. *United States v. Robinson*, 336 F.3d 1293, 1296 (11th Cir. 2003). As noted above, close questions are decided in the executing officers' favor. *Blake*, 868 F.3d at 975. Ultimately, the Court's task to determine, based on the totality of the circumstances, whether a reasonably well-trained officer would have relied upon the warrant, not whether the warrant was sufficient. *United States v. Taxacher*, 902 F.2d 867, 872 (11th Cir. 1990).

As discussed above, the warrant was supported by an affidavit that outlined a nexus between the darkweb site, Defendant's Coinbase account, and Defendant's home. The affidavit detailed when and how Defendant purchased a subscription to the darkweb site and it described the site's contents, the sophisticated steps required to navigate to it on the darkweb, and how those steps mask IP addresses. In short, the 32-paragraph affidavit was not so bare-bones and conclusory that no

officer could have reasonably relied on it. Accordingly, despite the deficiencies Defendant has asserted, the affidavit was not so lacking in indicia of probable cause that reasonable reliance was impossible.

4. Conclusion

For the foregoing reasons, the Court should deny Defendant's Motion to Suppress.

Respectfully submitted,

RYAN K. BUCHANAN
United States Attorney

/s/THEODORE S. HERTZBERG
Assistant United States Attorney
Georgia Bar No. 718163

Certificate of Service

The United States Attorney's Office served this document today by filing it using the Court's CM/ECF system, which automatically notifies the parties and counsel of record.

July 5, 2023

/s/ THEODORE S. HERTZBERG

THEODORE S. HERTZBERG

Assistant United States Attorney